この資料は Cisco 侵入防御システム（IPS）の検知時のアクション オーバーライドによって引き起こされる潜在的な問題を記述し、インストールを調整し、解決する推奨事項を提供したものです。

> **注** 検知時のアクション オーバーライドはリスク評価した上で基づいてシグニチャでとられるグローバル な処置です。 あらゆるグローバルコンフィギュレーションと同様に、コンフィギュレーション変更および付加との大きい注意を奪取 して下さい。

検知時のアクション 上書きする問題

説明

検知時のアクション オーバーライドはシグニチャ イベントにそのイベントが範囲を評価する規定された リスクの内で下るとき追加操作を追加します。 検知時のアクション オーバーライドを注意深く使用して下さい。 Iif 頻繁に引き起こされる イベントのための範囲を評価する広いリスクで上書きするを（IP 口ギング操作のような特に特定、高い操作、）、問題を引き起こすかもしれません作成します。

影響

余分イベント ストアに一般的に関連付けられます Command Line Interface （CLI）および Cisco IPS Device Manager （IDM）のような管理アクセス ツールへのセンサーの CPU使用率が高い状態および一般の無理解と書きます。

IP 口ギング操作およびファイル 記述子

ファイル 記述子はファイルのハンドルを得るためにプログラムによって使用されるデータ構造です; よく知られている な 記述子は規格、標準出力および標準 エラーのための 0,1,2 です。 ファイル 記述子はプロセスが新しいファイルかソケットを開くとき作成されます。

口グ攻撃者パケット、ログ ペア パケット、またはログ対象パケットのような IP 口ギング操作のための検知時のアクション 上書きするを作成すれば、これはファイル 記述子のプールを排出するかもしれません; 全面的なセンサー パフォーマンスは否定的に影響を受けるかもしれないし、センサーは適切に機能しないかもしれません。

SNMPトラップ操作および検知時のアクション オーバーライド

要求 snmp トラップの一つのアクションだけまたあるシグニチャはイベント ストアに書かれている警告イベントを生成します。 このように、簡易 ネットワーク 管理 プロトコル （SNMP） トラップ操作の余分な発生はまた生成 しますアラート操作を余分と見られる同じ問題を引き起こすかもしれません。

ノーマライザー エンジン シグニチャのための操作

ノーマライザー シグニチャにイベント ストアを書く（のようなアラート、要求 snmp トラップ、またはログ操作を生成 して下さい）引き起こす操作を追加しないで下さい。 これはすべての 1200-1330 範囲にシグニチャ ID を加えます。

簡潔なトラブルシューティンングのシナリオを除いて、ノーマライザー エンジン シグニチャのために検知時のアクション オーバーライドを使用しないで下さい。 これは特に問題となりますで:

- 非常にフラグメント化された IP シナリオ（1200 範囲 シグニチャによる）
- 重く故障中の（ooo） TCP シナリオ（1300 範囲 シグニチャ）

たとえば、検知時のアクション 上書きするは各 ooo TCPパケットのためのイベント ストアへの書を引き起こすリソースおよび利用問題を引き起こす場合があります。

0-100 のリスク評価の検知時のアクション オーバーライド

一般に低い定格が失敗の危険がある状態にセンサーをある特定の状況では置くことができるので、0-100 のリスク評価の検知時のアクション オーバーライドを避けて下さい。

メタ コンポーネント シグニチャは頻繁に表面上は良性の（および公有地）トラフィック の 種類で起動 します。 メタ シグニチャは親メタ シグニチャがアラートを始動させる前に引き起こすために 1つ以上のメタ コンポーネント シグニチャの組み合せを探します。 メタ コンポーネント シグニチャに、デフォルトで、それらと関連付けられる操作がありません; これはそれらがよくあるトラフィックで頻繁に一致するので計画的です。 メタ コンポーネント シグニチャに 15 のデフォルト ベース リスク評価があります。 検知時のアクション 上書きするのこれらのシグニチャ一致のキャプチャを除くために、Cisco は検知時のアクション 上書きするを作成するとき 25 より下部のを評価するリスクを使用しないことを推奨します; すなわち、リスク評価は 25-100 の下でないはずです。

IPS 利用を確認して下さい

コマンド

> **注** このセクションで使用されるコマンドに関する詳細を得るために Command Lookup Tool（登録ユーザのみ）を使用して下さい

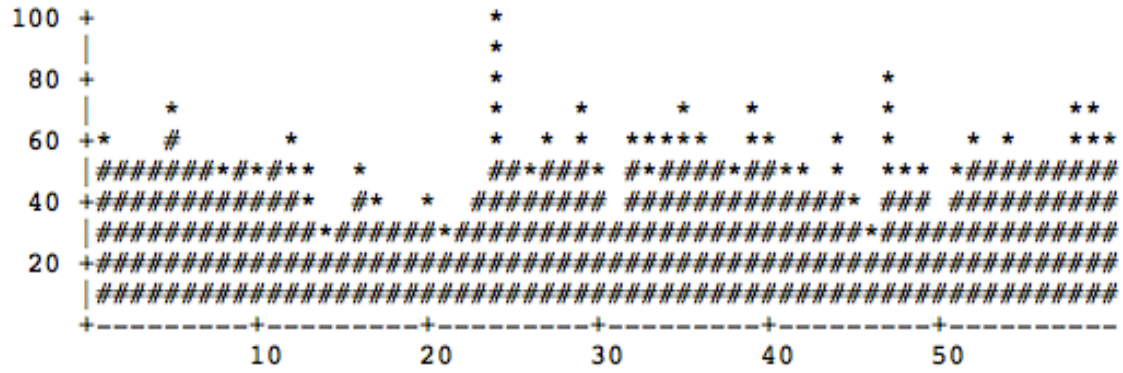
インスペクション ロード パーセントを探すために CLI の **show statistics バーチャル センサー** コマンドを入力して下さい:

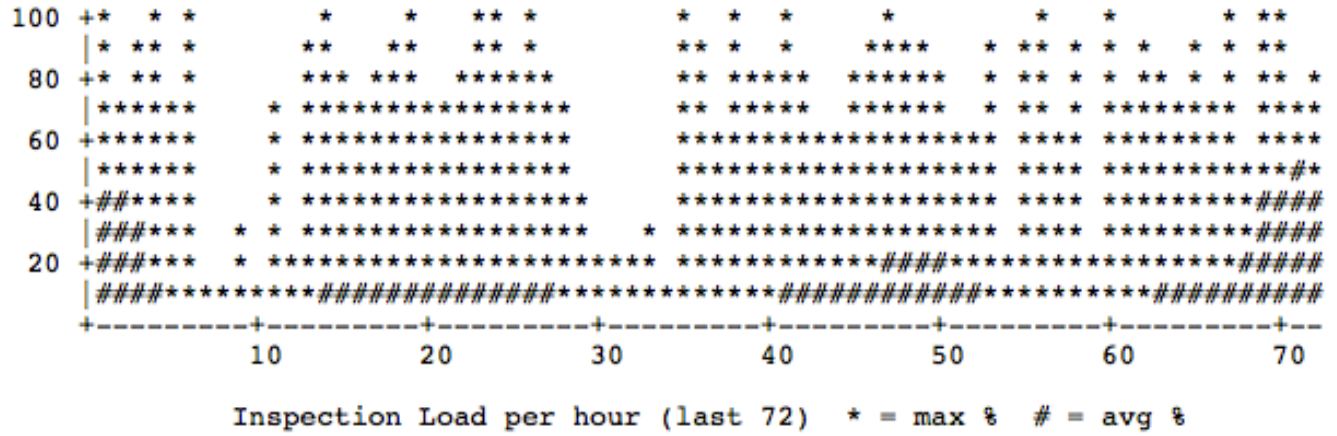
```
sensor# show statistics virtual-sensor | inc Load
Processing Load Percentage = 100
```

IPS バージョン 7.0(8)E4 および 7.1(6)E4 では、**提示インスペクション ロード** コマンドは追加されました:

```
sensor#  show inspection-load history
sensor 10:17:57 UTC Mon Apr 05 2013
```

これはそのコマンドからの出力例です:





非常に高負荷パーセントは（90% またはより高い）検知時のアクション オーバーライドによって引き起こされる余分なイベントがあることを示すかもしれません。 更にこの可能性を確認するために口グオンします順序を参照して下さい。

ログ

余分な検知時のアクション オーバーライドの主要なインジケータは例 main.log このファイルに見られるように、ラップする急速なイベント ストアです:

```
sensor#  show inspection-load history
sensor 10:17:57 UTC Mon Apr 05 2013
```

一般に、頻繁により発生するイベント ストア ラップは 1時間に1度問題を示唆するかもしれません。 あるシナリオでは、ラップは分以内の発生するかもしれない何回もほど余分です。 プラットフォームの全体的なパフォーマンス性能ケイパビリティのような多くの変数が、考慮するためにあります。

トラブルシューティング

どのようなイベント、トラフィック、または操作検知時のアクション 上書きする問題に引き起こしているか判別して下さい。 それは生成 アラート、IP 口ギング、ノーマライザー シグニチャ、またはメタ コンポーネント シグニチャですか。

- それが「話好きな」シグニチャであり、シグニチャを作成したらイベントのための false positive を判別したら、検知時のアクション フィルタ（EAF）を書いて下さい。
- IP 口ギングに関しては、Cisco は避けか、EAFs をまたは慎重に危険性の完全な知識と使用

し、EAFs を推奨します。
- ノーマライザー シグニチャおよびメタ コンポーネント シグニチャは一時トラブルシューティングのシナリオを除いてアラート操作がないはずです。

関連情報

- 検知時のアクション オーバーライドの設定
- IPS コンフィギュレーション ガイド
- テクニカルサポートとドキュメント - Cisco Systems